临澧县科技和工业信息化局

关于加强工业控制系统信息安全风险防控的通知

各相关单位、各相关企业：

近日，据报道，乌克兰电力系统遭受黑客钓鱼邮件攻击，造成严重损失，该事件是一次典型的针对工业控制系统的网络信息安全事件，须引起我县工业控制系统运营单位及相关部门的高度重视。根据省、市经信委的要求，请各单位认真对照相关文件和国家标准，加强工业控制系统的安全防护和检查评估工作。

附件：工业和信息化部电子科学技术情报研究所工业控制系统信息安全风险提示

临澧县科工局

2016年3月22日

工业控制系统信息安全风险提示

2016年第 1 期（总第 6 期）　　2016 年 1 月 26 日

乌克兰电力系统遭黑客钓鱼邮件攻击
我国工业企业需加强防范

近日，外电报道，2015 年 12 月 23 日，乌克兰电力系统遭受黑客攻击，导致伊万诺-弗兰科夫斯克地区大约一半的家庭停电 6 小时。此次攻击事件是由黑客通过钓鱼邮件等社会工程学方式，将可远程访问并控制工控系统的 BlackEnergy 恶意软件植入了乌克兰电力部门，造成电网故障。该事件的攻击方式和攻击工具具有先进的 APT 特征，完全具备了直接攻击工业控制系统主机、网络和软硬件的能力。据美国工业控制系统网络应急响应小组最新统计，钓鱼邮件攻击方式已成为工业控制系统网络攻击的主要手段，我国工业控制系统运营单位及相关主管部门需引起高度重视。

建议工业控制系统运营单位结合自身情况，及时采取以下消减措施：1. 做好网络分区与边界隔离管理，避免企业管理层的恶意软件渗透到生产控制网络；2. 加强企业网络安全

防护管理，部署防钓鱼攻击、恶意软件检测等 APT 安全防护措施；3. 加强移动介质使用管理，禁止不必要的外接设备或建立严格的移动介质使用流程，阻断潜在的攻击路径；4. 推动主机设备的补丁升级管理，及时修补主机系统存在的安全漏洞，并关闭不必要的应用和服务，避免恶意软件的利用；5. 提升员工的网络安全意识，避免攻击者利用社会工程学对工控系统实施入侵攻击。

编制单位：工业和信息化部电子科学技术情报研究所

发送：各地工业和信息化主管部门、有关国有大型企业、有关工业控制系统厂商

抄送：工业和信息化部信息化和软件服务业司

（联系人：李耀兵 010-88683438）